ABSTRACT OF THE DISCLOSURE

The present invention provides an apparatus and method for performing cryptographic operations on a plurality of input data blocks within a processor. In one embodiment, an apparatus for performing cryptographic operations is provided. The apparatus includes a cryptographic instruction, keygen logic, and execution logic . The cryptographic instruction is received by a computing device as part of an instruction flow executing on the computing device. The cryptographic instruction prescribes one of the cryptographic operations, and also prescribes that a user-generated key schedule be employed when executing the one of the cryptographic operations. The keygen logic is operatively coupled to the cryptographic instruction. The keygen logic directs the computing device to load the user-generated key schedule. The execution logic is operatively coupled to the keygen logic. The execution logic employs the user-generated key schedule to execute the one of the cryptographic operations.